

Amendments to the Claims:

The listing of the claims will replace all prior versions, and listings, of claims in the application:

Listing of the Claims:

1. (Original) A device for controlling access to a resource, access being provided through a host device having a USB bus, the device comprising:

(a) an input for receiving a request to access the resource;

(b) a flash memory device for storing at least one permission for determining access to the resource;

(c) a flash memory controller for controlling said flash memory device;

(d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, access to the resource is provided, and alternatively if said at least one permission does not include a type of access requested in said request, access to the resource is not provided; and

(e) a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from said processor.

2. (Original) The device of claim 1, wherein the device is implemented as a programmable ASIC.

3. (Original) The device of claim 1, wherein access is determined according to a biological parameter of a user, the device further comprising a biometric detection device for detecting said biological parameter of the user and for determining whether the user has said at least one permission to access the stored data, said biometric detection device being connected to said processor.

4. (Original) The device of claim 3, wherein said biometric detection device further comprises:

(i) a sample collector for collecting said biological parameter of the user; and (

ii) a software module for analyzing said biological parameter to determine whether the user has said at least one permission to access the resource.

5. (Original) The device of claim 4, wherein said biometric detection device further comprises:

(iii) a memory device for storing said software module and at least one previously collected biological parameter of the user; and

(iv) a data processor for operating said software module.

6. (Original) The device of claim 5, wherein said biological parameter of the user is a fingerprint of the user.

7. (Original) The device of claim 1, further comprising:

(f) a RAM component for storing data for performing said at least one instruction of said data processor.

8. (Original) The device of claim 1, further comprising:

(f) a cryptographic chip for encrypting and decrypting data.

9. (Original) The device of claim 8, wherein said cryptographic chip performs an authentication process.

10. (Original) The device of claim 8, wherein said cryptographic chip emulates a smart card.

11. (Original) The device of claim 10, wherein said cryptographic chip stores encrypted smart card data.

12. (Original) The device of claim 8, wherein said cryptographic chip performs encryption immediately upon receiving a command from said data processor.

13. (Original) The device of claim 12, wherein said cryptographic chip creates a cryptographic signature with a hash immediately upon receiving a command from said data processor.
14. (Original) The device of claim 8, wherein said cryptographic chip further comprises a cryptographic chip memory for storing at least one cryptographic key and at least one cryptographic instruction for encrypting and decrypting data, such that said cryptographic chip forms a removable encryption engine.
15. (Original) The device of claim 14, wherein said encrypted data is stored on said cryptographic chip memory.
16. (Original) The device of claim 15, wherein said cryptographic chip memory is a separate flash memory device from said flash memory device.
17. (Original) The device of claim 15, wherein said cryptographic chip memory is said flash memory device.

Claims 18-50 (Canceled).